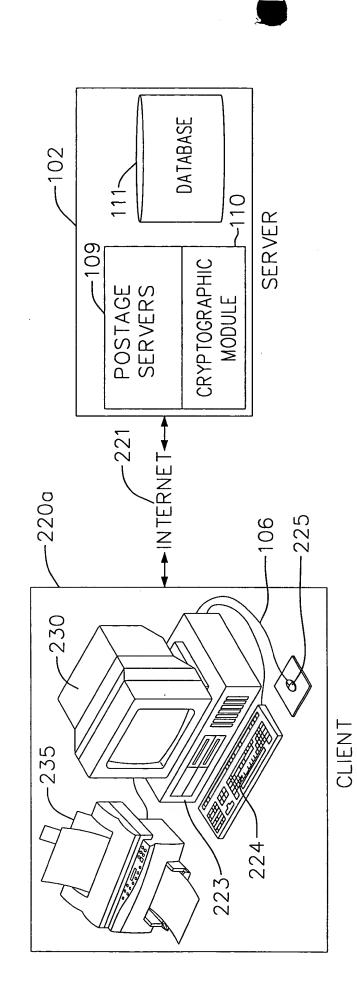
DOSCOPLE TOCHOLO





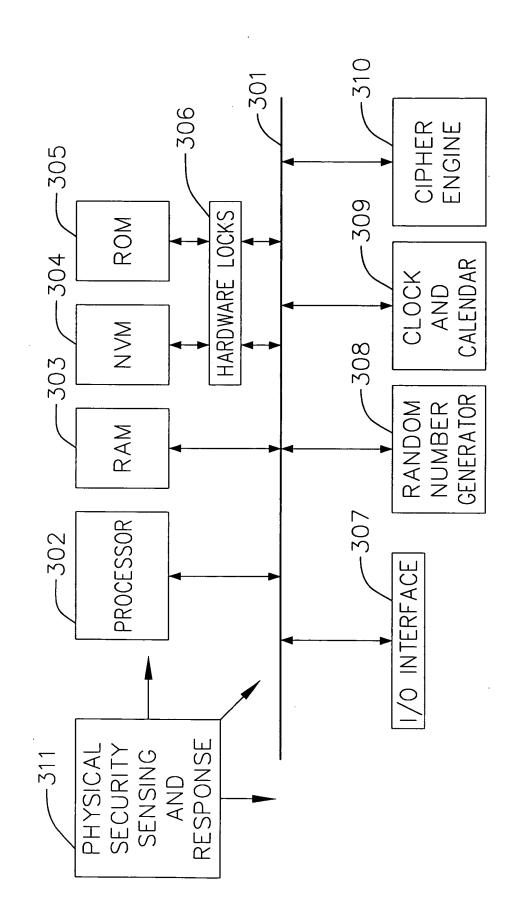
COMPOST INTEGS

FIG.2

222a 222m SERVER • • • SERVER 234 221 -233n LOCAL NETWORK INTERNET -235 -233a -232n 220n PRINTER COMM NETWORK, LINK -220a MONITOR 232a COMM ,231 230 227 MASS STORAGE MAIN MEMORY MONITOR VIDEO AMP 228 225 229 VIDEO MEMORY VIDEO AMP MOUSE 2 226 223 224 KEYBOARD CPU

APPROVED O.G. FIG.		
BY	CLASS	SUBCLASS
DRAFTSMAN		

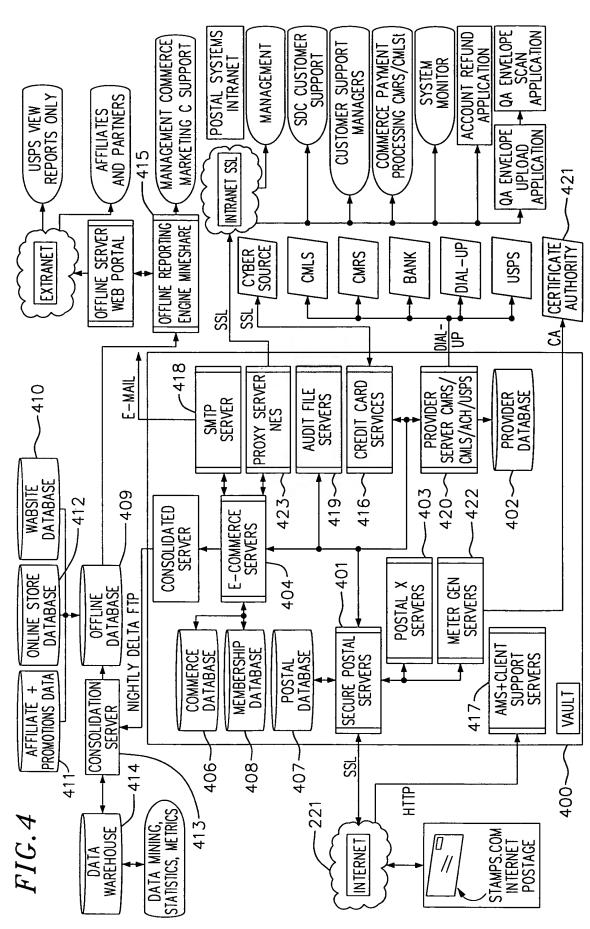
FIG.3



ĻŲ

įΞ

-4



APPROVED O.G. FIG CLASSISUBCLASS BY DRAFTSMAN

FIG.5

GENERATES A RANDOM, 64-BIT CHALLENGE CLIENT SOFTWARE

THE CHALLENGE IT SENT WITH COMPARES THE HMAC OF THE HMAC IT RECEIVES CLIENT SOFTWARE FROM THE PSD.

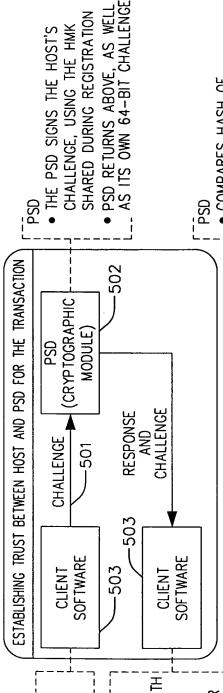
- HOST TRUSTS THE PSD FOR THIS TRANSACTION
- CHALLENGE TO AUTHENTICATE HOST RETAINS PSD'S ITSELF TO THE PSD

505-

CUSTOMER'S ASCENDING AND SIGNS CHALLENGE THAT THE PSD SENT, AND ALSO THE **-OCAL RECORD OF THE** DESCENDING REGISTERS. SENDS THIS TO PSD. CLIENT SOFTWARE

SENDS CLEARTEXT OF THE RANSACTION MESSAGE. CHALLENGE AND THE

SENDS AN HMAC OF ALL OF THE ABOVE, USING SHARED



CALCULATION OF THE SAME. WAS NOT TAMPERED WITH. THIS ENSURES MESSAGE RESPONSE WITH LOCAL COMPARES HASH OF

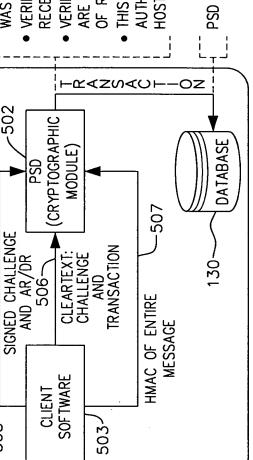
ESTABLISHING TRUST BETWEEN PSD AND HOST FOR THE TRANSACTION

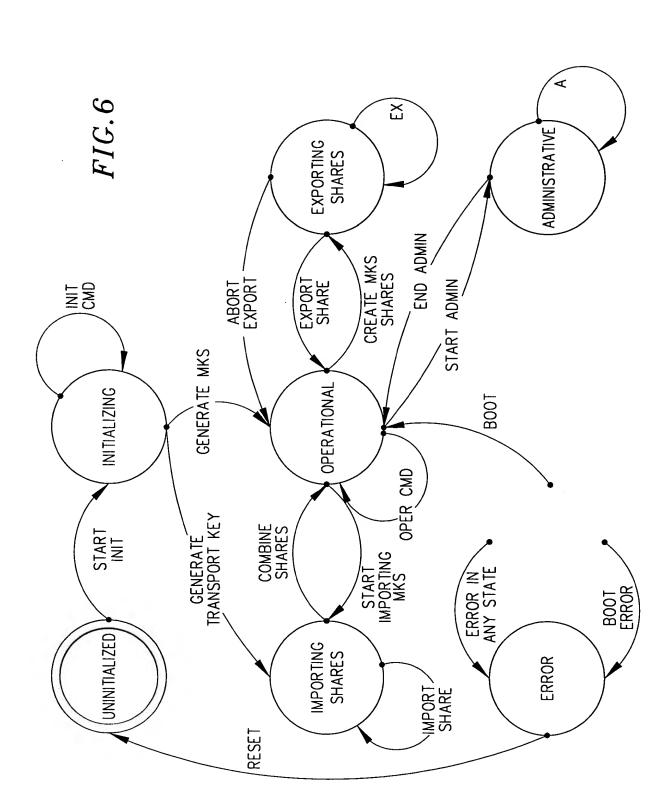
502

RECEIVED IS CHALLENGE SENT. VERIFIES HOST'S REGISTERS VERIFIES CHALLENGE

ARE SAME AS LOCAL DATA OF REGISTERS.

THIS ABOVE TWO STEPS AUTHENTICATE THE PSD PERFORMS TRANSACTION





:= -3

:5

-4

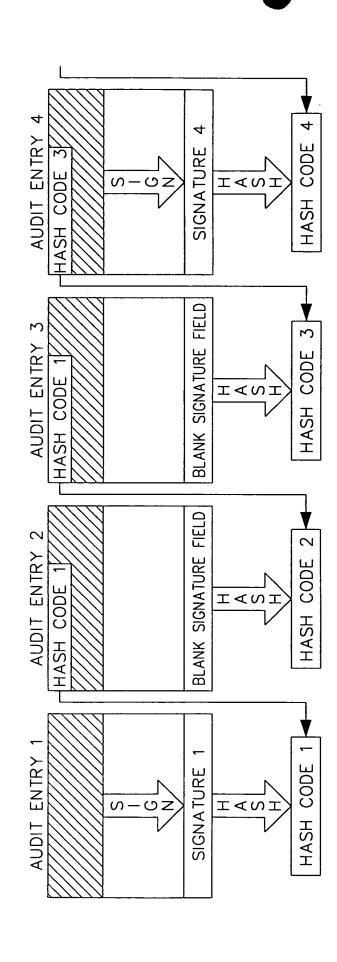
APPROVED O.G. FIG.

BY

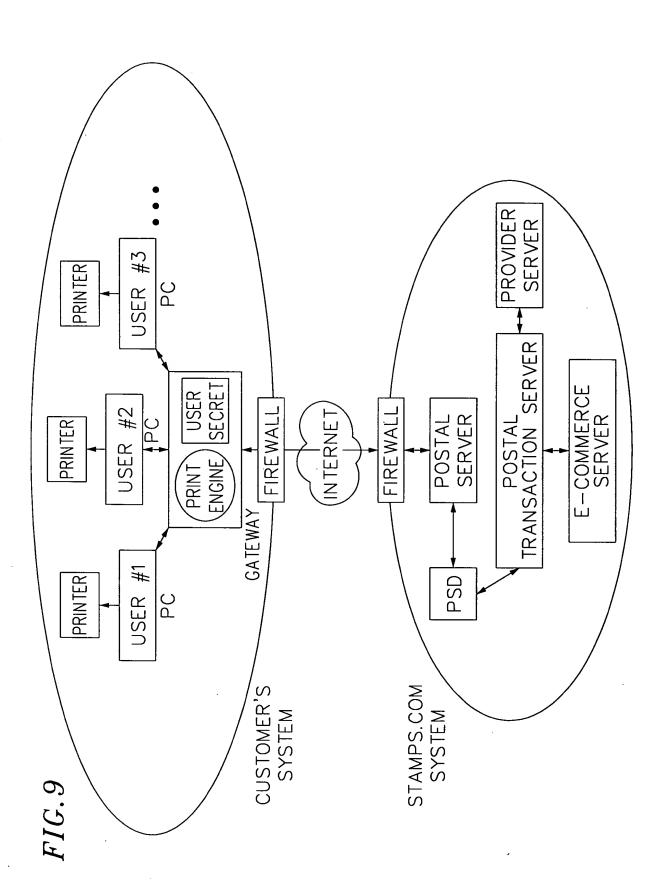
CLASS SUBCLASS

DRAFTSMAN

FIG. 7







il lada

ļ.4 ļņ

FIG. 10

